An Epidemic Model of Mobile Phone Virus

Hui Zheng[1], Dong Li[2], Zhuo Gao[3]
[1]*Network Research Center, Tsinghua University, P. R. China*
zh@tsinghua.edu.cn
[2] *School of Computer Science and Technology,*
Huazhong University of Science and Technology, P. R. China
lidong@hust.edu.cn
[3]*Department of Physics, Beijing Nomarl University, P. R. China*
zhuogao@bnu.edu.cn

Abstract

Considering the characteristics of mobile network, we import three important parameters: distribution density of mobile phone, coverage radius of Bluetooth signal and moving velocity of mobile phone to build an epidemic model of mobile phone virus which is different from the epidemic model of computer worm. Then analyzing different properties of this model with the change of parameters; discussing the epidemic threshold of mobile phone virus; presenting suggestions of quarantining the spreading of mobile phone virus.

Keywords: Mobile Phone Virus, Epidemic Model, Security of Wireless Network, Bluetooth, Smart Phone.

1. Introduction

The first computer virus that attacks mobile phone is VBS. Timofonica which was found on May 30, 2000 [1]. This virus spreads through PCs, but it can use the message service of moviestar.net to send out rubbish short messages to its subscriber. It is propagandized as mobile phone virus by the media, but in fact it's only a kind of computer virus and can't spread through mobile phone which is the only attacked object. Cabir Cell Phone Worm which was found on June 14, 2000 is really a mobile phone virus [2]. It spreads from one cell phone to another by Bluetooth. Now it is found in more than 20 countries and has more than 7 variants. Cabir has the characteristic of initiative spreading and this pattern will be mostly adopted by "mobile phone virus" in the future.

Table 1 lists the comparison between configuration of smart phone and computer. This table presents the most advanced desk-top computer configuration in 1998 and 1999. Generally, it takes 2 to 3 years for computer with the most advanced configuration to become popular. That is to say, when the Code Red Worm broke out in 2001, common hardware of computers in Internet was as same as the configuration in table 1. With the comparison in table 1, we can see that smart phone presently has already possessed hardware condition for computer virus spreading.

Table 1. Hardware comparing between smart phone and desk-top personal computer

Hardware	2005(dopod 828)	1998 PC	1999 PC
CPU	Intel 416MHz	Pentium Ⅱ 333MHz	Pentium III 450MHz[3]
Memory	128M	32M	64M
Hard Disk	2G~8G	2G	6G

The development and popularization of smart phone are both very fast. According to the statistics of ARC, in 2004 the sum of smart phone is 27,000,000, accounting for 3% of the global amount of mobile phones. IDC estimates that the sum of smart phone will reach up to 130,000,000 by 2008 and account for 15% of the global amount of mobile phones [4]. So we should pay much attention to the security of smart phone.

In this paper, "smart phone" is one smart mobile terminal device with the integrated ability of data transmission, processing and communication; "mobile phone virus" is a malicious code that can spread through all kinds of smart mobile terminal devices. As to the security research, though we can refer to the security research results in MANETs (Mobile Ad Hoc Networks), MANETs and Sensor network emphasize that resource is finite and all the problems about application and security should be restricted to this precondition [12]. Smart mobile terminal device emphasizes that resource is abundant, even possess the same computing ability as desk-top personal computer. So for these two security problems, the starting points of research are different. Recently, paper [5] demonstrates that traditional epidemic model of computer virus can't be applied to virus spreading in

mobile environment and the epidemic model when the mobile phone moves with variable velocity is also discussed. But in a small area, uniform motion accords with the sport law of human being preferably. What's more, some important parameters such as distribution density and signal coverage radius are not imported to the model. Paper [6] compares to the required condition of virus spreading in computer and gives the corresponding required condition of virus spreading in MANETs by simulation.

This paper first discusses several spreading modes of mobile phone virus; The second section builds the epidemic model of mobile phone virus which imports 3 parameters: moving velocity, signal coverage radius and distribution density; The third section analyses some relevant characteristics of this model; the fourth section compares the epidemic model of mobile phone virus with the epidemic model of Internet worm and discusses the threshold of mobile phone virus breaking out. At last, we make some discussions.

2. The spreading way of mobile phone virus

Though paper [7~8] presents many examples of "mobile phone virus", many of them are not able to spread, so they are not real mobile phone virus. According to analysis of all kinds of epidemic malicious codes which have been found, such as Cabir [2], Commwarrior [9], Brador [10], Skull [11] etc, we can define mobile phone virus: it is a piece of data or program that spreads among smart mobile terminal devices by the communication interfaces and can influence the usage of handset or leak out sensitive data. Through the analysis of spreading way, we can conclude table 2:

Table 2. Spreading way of mobile phone virus

Wireless spreading channel	Spreading distance	Spreading direction	Way of discovering neighbor nodes	Relay (Yes or No)
GPRS/CDMA 1XRTT	1000m	Non-directional	Appointed	Yes
Wi-Fi(802.11)	100m	Non-directional	Appointed	Yes
Bluetooth	10m	Non-directional	Automatic	No
IrDA	1m	Directional	Automatic	No

For the mobile phone virus that can spread by MMS and E-mail, it can transmit data by GPRS and Wi-Fi; for the mobile phone virus that spread by electronic file, it can transmit data by Bluetooth and IrDA. Although there are four wireless transmission ways, some need relay nodes or directional angle, so Bluetooth is the best choice for virus writer.

In this model, we mainly consider those mobile phone viruses that spread through Bluetooth. For other ways of transmission, we will build the model in other papers.

3. The epidemic model of mobile phone propagating

Supposing mobile phone has two statuses: Susceptible and infected. The infected will come back to susceptible with certain probability. In table 3, we define some symbols:

Table 3. Symbol definition

Symbol	Instructions
Ω	moving space of mobile phone (2-dimmension)
ρ	distribution density of mobile phone (uniform distribution)
v	moving velocity of mobile phone (uniform velocity)
r	coverage radius of Bluetooth signal
I	The number of virus in mobile phone at time t
β	epidemic rate of mobile phone virus propagating
δ	resuming rate of the infected

Then we can build the epidemic model of mobile phone virus:

$$\frac{dI}{dt} = I \cdot ((\pi \cdot r^2 + 2 \cdot r \cdot v) \cdot \rho - 1) \cdot \frac{\Omega \cdot \rho - I}{\Omega \cdot \rho} \cdot \beta - \delta \cdot I$$

Suppose:

$$a = (\pi r^2 + 2rv)\rho\beta - \beta - \delta ,$$

$$b = \frac{(\pi r^2 + 2rv)\rho\beta - \beta}{\Omega\rho} ,$$

Then the differential equation is：

$$\frac{dI}{dt} = aI - bI^2 ,$$

The solution is：

$$I = \frac{ae^{at+c}}{1 + be^{at+c}} ,$$

For $I(t_0)$, the initial value of c is a constant.

We can conclude from the solution: if $a < 0$, then $I \to 0$, and if $a > 0$, then $I \to \frac{a}{b}$.

4. Analysis of model properties

The changes of model properties with changes of different parameters are researched. Table 4 presents the range of parameters.

Table 4. The range of parameters

Symbol	Instruction	Range
Ω	moving space of mobile phone (2-dimmension)	1000m * 1000m
ρ	distribution density of mobile phone (uniform distribution)	0.001~0.1/m^2
v	moving velocity of mobile phone (uniform velocity)	2m/s
r	coverage radius of Bluetooth signal	10m
β	epidemic rate of mobile phone virus	0.75
δ	resuming rate of infected	0.025
I_0	The number of initial infected mobile phones	5

4.1. Influence of distribution density to virus spreading

The connotative subject condition of equation is $\rho > \frac{1}{(\pi \cdot r^2 + 2 \cdot r \cdot v)}$, mobile phone virus is able to spread when this condition is satisfied. Figure 1 shows the relationship between distribution density and infection percentage. When the subject condition is not satisfied, infection percentage is 0; when the subject condition is satisfied, the infection percentage is very sensitive to the change of distribution density, the small change of distribution density can lead to great improvement proportion of the infected.

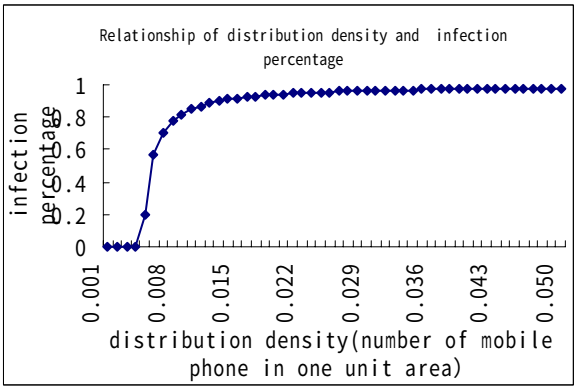

Figure 1. Relationship of distribution density and infection percentage

Figure 2 is the relationship between distribution density and spreading time. It shows the influence of distribution density to moving velocity. Mobile phone virus can't spread when distribution density is small. Spreading time that the infection of mobile phone virus gets to equilibrium reflects the spreading velocity of virus. From these we can see that spreading velocity is very sensitive to the change of distribution density.

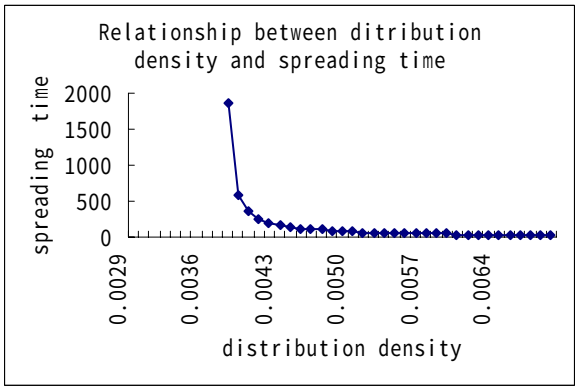

Figure 2. Relationship between distribution density and spreading time

4.2. Influence of coverage radius to virus spreading

Considering the range of coverage radius of Bluetooth signal r varies from 5m to 15m. Distribution density of mobile phone is 0.005. Figure 3 is the relationship of coverage radius and percentage of the infected, which presents the influence of coverage radius to virus spreading.

From these we can see that mobile phone virus can't spread when coverage radius is very small. If it spreads, the infection percentage will change with coverage radius.

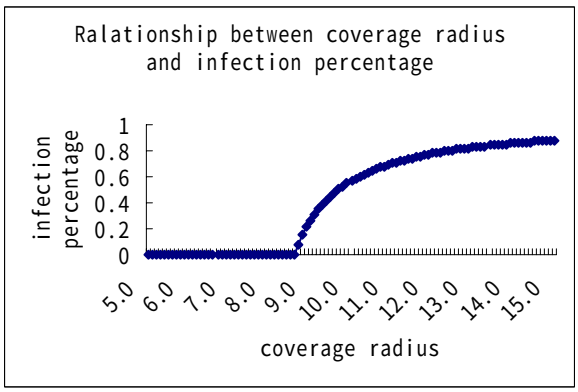

Figure 3. Relationship between coverage radius and infection percentage

Figure 4 is the relationship between coverage radius and spreading time, it presents the influence of coverage radius to spreading velocity. Virus can't spread when coverage radius is very small. Spreading velocity is very sensitive to the changes of coverage radius.

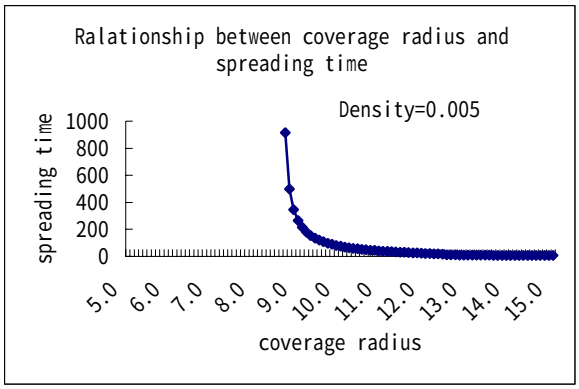

Figure 4. Ralationship between coverage radius and spreading time

4.3. Influence of moving velocity to virus spreading

Assuming distribution density of mobile phone is 0.0035, the range of moving velocity is 1m/s~30m/s, figure 5 is the relationship between moving velocity and infection percentage, it presents the influence of moving velocity to the spreading of mobile phone virus. For the small distribution density of mobile phone and typical coverage radius, speeding the moving velocity can result in the spreading of the virus which can't spread before.

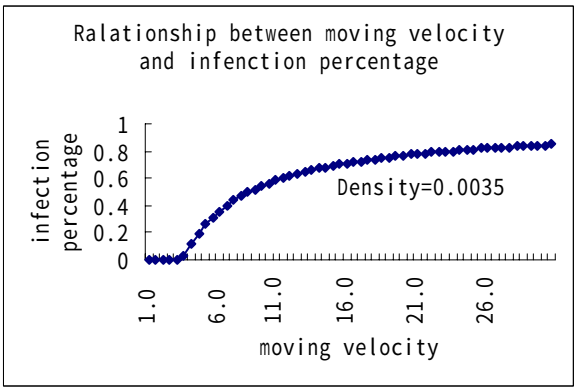

Figure 5. Relationship between moving velocity and infection percentage

Figure 6 is the relationship between moving velocity and spreading time. It presents the influence of moving velocity to spreading velocity. From this figure we can see that increasing of moving velocity can speed up the spreading of virus.

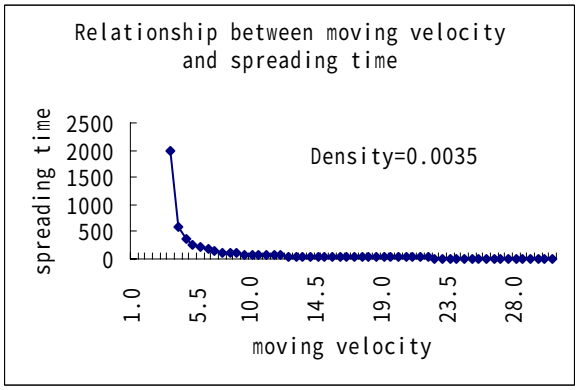

Figure 6. Relationship between moving velocity and spreading time

The time that virus file transfers from one mobile phone to another is T_f , the discussion above supposes that the moving of mobile phone has no influence to virus spreading. If we take into account the influence of moving velocity of mobile phone, we can add one subject condition: $v < \frac{r}{T_f}$. When this condition is satisfied, virus can spread. When this condition is not satisfied, that is to say, mobile phone moves too fast, then the time that virus stay in the coverage area of signal is too short, virus can't spread.

5. Results of comparison with epidemic models of worm

The corresponding epidemic model of worm in computer network can be expressed as [13]:

$$\frac{dI}{dt} = I \cdot (\Omega \cdot \rho - I) \cdot \beta - \delta \cdot I$$

In computer network, $\Omega \cdot \rho$ is the sum of computer and it is a fixed value in short time. The threshold of its spreading is: $\frac{\delta}{\beta} < \Omega \cdot \rho$. If this condition is satisfied, worm can spread. This condition can be satisfied easily.

Different from the spreading threshold of computer virus, the spreading threshold of mobile phone virus is subject to coverage radius of wireless signal, moving velocity and distribution density. According to the stabilized solution of differential equation, we can see:

if $a < 0$, then $I \to 0$;

for

$$a = (\pi r^2 + 2rv)\rho\beta - \beta - \delta,$$

we can get a new threshold:

$$\frac{\delta}{\beta} < (\pi \cdot r^2 + 2r \cdot v) \cdot \rho - 1.$$

When this condition is satisfied, virus will break out; if this condition is not satisfied, virus can't break out.

From these we can see: the condition that mobile phone virus breaks out is much more rigorous than worm in computer network. So the probability of that mobile phone virus breaks out in large area is very small, but it is possible in local area.

6. Conclusions

Because of the mobility, mobile phone has some relevant characteristics: moving velocity, moving scope etc, which make the epidemic model of mobile phone virus very different from the model of computer virus and worm.

We can make use of stochastic mobile model (such as Random Waypoint model, Random Direction model [14]) to build spreading model of mobile phone virus. But these stochastic models have some limitations and can't accord with the fact preferably. For simplification of this problem, we build this model with uniform motion.

Through the analysis of this model, we can conclude some measures of quarantining mobile phone virus: reducing coverage radius, such as reducing signal power, or interfering signal etc; decreasing moving velocity, such as restricting the flowage of person; lessening distribution density of mobile phone, such as controlling the moving area of someone with mobile phone; these measures have distinct differences with the usual ways of quarantining mobile phone virus spreading.

Acknowledgement

This work is supported in part by National Science Foundation of China under contract 60203004; by High-Tech Program (863) of China under contract 2003AA142080. Points of view in this document are those of the authors and do not necessarily represent the official position of Tsinghua University, Huazhong University of Science and Technology, or Beijing Nomarl University.

References

[1] Symantec. VBS.Timofonica. http://www.symantec.com/avcenter/venc/data/vbs.timofonica.html

[2] Symantec. SymbOS.Cabir. http://securityresponse.symantec.com/avcenter/venc/data/symbos.cabir.html

[3] History of Computer Development. http://www.net130.com/2004/5-28/20344-4.html. (in Chinese)

[4] Neal Leavitt. Mobile Phones, The Next Frontier for Hackers. IEEE Computer, 38(4): 20-23, 2005.

[5] James W. Mickens, Brian D. Noble. Modeling Epidemic Spreading in Mobile Environments. WiSE'05, September 2nd, 2005, Cologne, Germany.

[6] Robert G. Cole, Nam Phamdo, Moheeb A. Rajab, Andreas Terzis. Requirements on Worm Mitigation Technologies in MANETs. Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS'05).

[7] Shi-an Wang. Principle and Defense of Mobile Phone Virus. Journal of Dal ian Institute of Light Industry, 23(1): 74-76, 2004. (in Chinese)

[8] Kai Li, Hao Chen. Virus Threats to GSM Mobile Phones. China Information Security, 7:226-228, 2005. (in Chinese)

[9] Mikko Hypponen, Jarno Niemela. F-Secure Virus Descriptions Commwarrior. A. March 7th, 2005.http://www.f-secure.com/v-descs/commwarrior.shtml

[10] Viruslist-Backdoor. WinCE.Brador, a Viruslist. Aug 5th, 2004. http://www.viruslist. com/en/viruslist.html?id=1984055

[11] Dan Ilet and Matt Hines. Skulls program carries Cabir worm into phones. Techrepublic. Nov 30th, 2004. http://techrepublic.com /5100-22_11-5471004.html

[12] Sang ho Kim, Choon Seong Leem. Security Threats and Their Countermeasures of Mobile Portable Computing Devices in Ubiquitous Computing Environments. ICCSA 2005, LNCS 3483, pp. 79 – 85, 2005.

[13] J. Kephart and S. White. Directed-graph epidemiological models of computer viruses. In Proceedings of the IEEE Computer Symposium on Research in Security and Privacy, pages 343–359, May 1991.

[14] Bettstetter, H. Hartenstein, and X. Perez-Costa. Stochastic Properties of the Random Waypoint Mobility Model. ACM/ Kluwer Wireless Networks, 10(5):555–567, September 2004.